HOW TO SAVE ELECTRONIC EVIDENCE

INFORMATION SHEET FOR INTERVENORS

INTERVENOR'S ROLE: PROVIDING SUPPORT AND ASSISTANCE

New technologies constitute an especially powerful instrument for documenting cases where intimate partner violence is present in a couple. This can be accomplished using the geolocation feature or online chat platforms, photos, text messages, etc.

In your role as an intervenor, we recommend that you offer your support to the at-risk partner if they want to gather and save evidence. Doing so may cause anxiety and fear on the part of the at-risk partner, so they will need your support for their decision.

Be careful!
Since the violent partner may have access to the at-risk partner's accounts and devices where evidence is stored, the violent partner may be aware of the existence of such evidence. **Inform the at-risk partner of this possibility and support them in their decision.**

1 SUGGEST TO THE AT-RISK PARTNER THAT THEY SAVE ANY ELECTRONIC EVIDENCE

If they agree:

- Give the at-risk partner a copy of the information document entitled "How to Save Electronic Evidence: General Information Sheet" and explain the different options available to them if they want to gather and save electronic evidence.
- Make sure that the means used to gather and save evidence is SECURE.
- Point out that gathering and saving evidence does not necessarily guarantee that it will be admissible in court.

If they voice any fears:

- Point out that they can gather and save evidence even if they do not file a complaint.
- Respect their choice and do not pressure them.
- Let them know you are available if they change their mind.
- Ask them if they still want to receive the information document "How to Save Electronic Evidence: General Information Sheet."

2 MAKE SURE THAT THE AT-RISK PARTNER IS THE ONLY PERSON WHO HAS ACCESS TO THEIR ACCOUNTS

- ☐ The at-risk partner's cellphone account with their service provider should be under their own name.
- ☐ The at-risk partner should know the user name associated with their device (ex.: Apple ID, Google account).
- ☐ The at-risk partner should be the only person who knows their password and the only person able to connect to the username for their device.
- ☐ The at-risk partner should be the only person who has access to their social media accounts.
- ☐ The at-risk partner should be using two-factor authentication (2FA) on their cellphone to connect to their accounts (2FA or "two-factor authentication" provides an extra level of protection to make sure that the at-risk spouse is the only person who can access their accounts).
- ☐ Any authorized devices linked to the at-risk partner's username should be devices that the at-risk partner knows about and has under their own control (cellphone, tablet, iPod).
- ☐ If in doubt, the at-risk partner should reset their passwords and check the security information for their accounts.

To manage security for a **Google account**:
- https://myaccount.google.com

To manage security for an **Apple account**:
- https://appleid.apple.com

3 INFORM THE AT-RISK PARTNER ABOUT GOOD DOCUMENTATION PRACTICES

Where did you see the information?
On what platform (ex.: Messenger, Instagram, Snapchat, etc.)?

At what URL address?
The address of a hypertext site or page on the internet (ex.: http://www.lerobert.com).

Who did you have the exchange with?
The person's unique identifier on the platform.

When did you see the information?
Date, time, time zone.

The at-risk partner should record the information using the following format: *Conversation on [month] [day], [year] at [hour]:[minute] [a.m. or p.m.], between [person] and [person] on [platform]. Ex.: Conversation on May 12, 2019 at 8:30 a.m., between Paul and Louise on Facebook.*

If circumstances permit it, the at-risk partner should gather and save the evidence where it is. Do not delete it.

SQ-3619A (03-2021)

INFORMATION SHEET FOR INTERVENOR(S)

4 CHARACTERISTICS OF DIFFERENT PLATFORMS

	FACEBOOK MESSENGER	INSTAGRAM	SNAPCHAT
FEATURES	• Sending messages. • Making audio calls. • Making video calls.	• Sending messages. • Making video calls.	• Sending photos and videos. • Chatting. • Making audio calls. • Making video calls.
PERSISTENCE OF MESSAGES	Average	Average	Low
CHARACTERISTICS	Preserved messages. Possibility to delete messages from a common conversation.		Messages, photos and videos are deleted automatically. Items are deleted after they have been viewed twice. <u>Be careful!</u> The user is notified when a screenshot is taken.
OPTIONS ON MOBILE APPLICATION	Stories: Photos, videos published on the FB or Instagram account for 24 h. Vanish mode: Messages disappear once the conversation is closed. Secret conversation (only FB): • Encrypted. • Allows you to define the message deletion time.		Stories: Photos, videos published on the Snapchat account for 24 h. Change the deletion period of chats (max. 24h).
POSSIBLE OPTIONS FOR SAVING EVIDENCE	• Not deleting conversations. • Screenshots. • Archiving a conversation by masking it in the inbox. • Asking for the account archives. • Keeping documentation.	• Screenshots. • Keeping documentation. • Not deleting conversations. • Asking for the account archives.	• Using another device to take photos (this avoids the issue of sending a notification to the violent partner). • Save manually chat messages by pressing each item. • "My Eyes Only" feature is reserved for items you want to keep for yourself with a secret code. • Keeping documentation.
DOCUMENTATION	https://www.facebook.com/help/	https://help.instagram.com	https://support.snapchat.com

RESSOURCES AVAILABLE FOR HELP

TO OBTAIN SUPPORT

SOS VIOLENCE CONJUGALE
(24/7, throughout Quebec)
1 800 363-9010

CAVAC
(office hours)
1 866 532-2822

TO REPORT INTIMATE PARTNER VIOLENCE

THE POLICE FORCE
serving your municipality

SÛRETÉ DU QUÉBEC
911 (310-4141 or *4141 for municipalities not served by 911)